

Falha na consulta de conformidade MDM do ISE 3.2 devido à supressão do cliente e a um defeito de software

Contents

Problema

Alguns pontos de extremidade autenticados via EAP-TLS no Cisco Identity Services Engine (ISE) não recebem um status de conformidade do Microsoft Intune de forma intermitente, mesmo que sejam mostrados como compatíveis no painel do Intune. Como resultado, esses endpoints atingem uma política de autorização sem fio padrão, em vez da política de conformidade com a postura ou de não conformidade com a postura esperada. Os endpoints afetados não mostram os atributos de conformidade do gerenciamento de dispositivos móveis (MDM) nos logs ao vivo do ISE ou nos relatórios de MDM externo, e o problema afeta apenas um subconjunto de clientes na implantação.

Os sintomas específicos observados incluem:

- Clientes anormais não têm logs no Relatório do ISE no Relatório de Gerenciamento de Dispositivos Móveis Externos.
- Clientes anormais não têm atributos como status de conformidade MDM ou status de conformidade do dispositivo nos detalhes do log ao vivo.
- Clientes anormais atingem a política de autorização 802.1x_EAP-TLS_toyotawifi sem fio em vez da política de conformidade com postura.
- As mensagens de erro nos logs estão mostrando "Falha ao conectar ao servidor MDM: 404 Não encontrado".

Ambiente

- Patch 6 da versão 3.2 do cluster de vários nós do Cisco ISE

- 8 nós do ISE no cluster, todos mostrando status verde
- 11.000 clientes com/sem fio integrados ao Microsoft Intune
- Os clientes usam a autenticação EAP-TLS (Machine Certificate)
- O ISE usa o endereço MAC do cliente para consultas ao Intune
- Todos os clientes têm status de conformidade no painel do Microsoft Intune
- O problema afeta alguns clientes, mas não todos

Resolução

O problema foi resolvido por meio dessas etapas.

Passo 1: Identificar a causa raiz

A análise dos logs do ISE revelou que os endpoints afetados têm uma ID de servidor MDM obsoleta, impedindo que as consultas MDM sejam executadas.

Os registros mostraram:

```
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MDMUtil -:::- M
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MdmServersCache -
2026-06-15 13:35:14,344 ERROR [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.pip.MdmPartnerPIPHandl
```

Além disso, descobriu-se que a implantação estava atingindo o bug da Cisco ID CSCwv51917, que afeta as pesquisas de conformidade de MDM quando o uso do endereço MAC tem um ID de servidor MDM antigo.

Passo 2: Solução temporária

Como uma solução temporária:

1.- Exclua o endpoint de Visibilidade de Contexto e autentique-o novamente. Isso foi observado para corrigir o problema de consultar o servidor MDM e obter o status de conformidade.

2.- Navegue até Visibilidade do Contexto.

3.- Selecione o endereço mac do ponto final e exclua-o.

4.- Autentique novamente o endpoint.

Passo 3: Resolução permanente - Atualização de software

A resolução permanente está sendo rastreada sob a ID de bug Cisco CSCwv51917.

Causa

Durante a autenticação, o ISE tenta consultar a referência de servidor MDM obsoleta, mas o objeto de servidor MDM correspondente não existe mais ou está inativo. Consequentemente, o ISE não recupera atributos de conformidade MDM do Intune.

Conteúdo relacionado

- [ID de bug Cisco CSCwv519173134](#)
- [Notas da versão do ISE 3.2 - Avisos resolvidos](#)
- [Aviso de fim da vida útil do ISE 3.2](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.